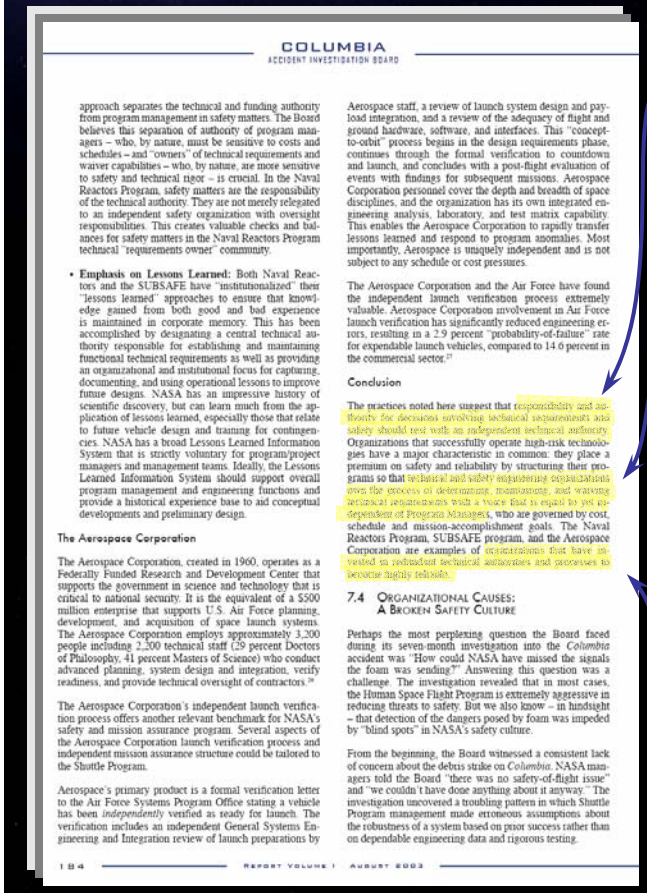
Putting Technical Authority into Practice
NASA Project Management Conference
03.22.05

Rex Geveden
Chief Engineer, NASA

Collier's, using the ideas and drawings of Werner von Braun depicting space "tugs" and Space Stations, fired the imagination of millions.
March 22, 1952

NASA Missions

The CAIB and Technical Authority



COLUMBIA
ACCIDENT INVESTIGATION BOARD

approach separates the technical and funding authority from program management in safety matters. The Board believes this separation of authority of program managers – who, by nature, must be sensitive to costs and schedules – and "owners" of technical requirements and waiver capabilities – who, by nature, are more sensitive to safety and technical rigor – is crucial. In the Naval Reactors Program, safety matters are the responsibility of the technical authority. They are not merely relegated to an independent safety organization with oversight responsibilities. This creates valuable checks and balances for safety matters in the Naval Reactors Program technical "requirements owner" community.

- **Emphasis on Lessons Learned:** Both Naval Reactors and the SUBSAFE have "institutionalized" their "lessons learned" approaches to ensure that knowledge gained from both good and bad experience is maintained in corporate memory. This has been accomplished by designating a central technical authority responsible for establishing and maintaining functional technical requirements as well as providing an organizational and institutional focus for capturing, documenting, and using operational lessons to improve future designs. NASA has an impressive history of scientific discovery, but can learn much from the application of lessons learned, especially those that relate to future vehicle design and training for contingencies. NASA has a broad Lessons Learned Information System that is strictly voluntary for program/project managers and management teams. Ideally, the Lessons Learned Information System should support overall program management and engineering functions and provide a historical experience base to aid conceptual developments and preliminary design.

The Aerospace Corporation

The Aerospace Corporation, created in 1960, operates as a Federally Funded Research and Development Center that supports the government in science and technology that is critical to national security. It is the equivalent of a $500 million enterprise that supports U.S. Air Force planning, development, and acquisition of space launch systems. The Aerospace Corporation employs approximately 3,200 people including 2,200 technical staff (29 percent Doctors of Philosophy, 41 percent Masters of Science) who conduct advanced planning, system design and integration, verify readiness, and provide technical oversight of contractors.[38]

The Aerospace Corporation's independent launch verification process offers another relevant benchmark for NASA's safety and mission assurance program. Several aspects of the Aerospace Corporation launch verification process and independent mission assurance structure could be tailored to the Shuttle Program.

Aerospace's primary product is a formal verification letter to the Air Force Systems Program Office stating a vehicle has been *independently* verified as ready for launch. The verification includes an independent General Systems Engineering and Integration review of launch preparations by Aerospace staff, a review of launch system design and payload integration, and a review of the adequacy of flight and ground hardware, software, and interfaces. This "concept-to-orbit" process begins in the design requirements phase, continues through the formal verification to countdown and launch, and concludes with a post-flight evaluation of events with findings for subsequent missions. Aerospace Corporation personnel cover the depth and breadth of space disciplines, and the organization has its own integrated engineering analysis, laboratory, and test matrix capability. This enables the Aerospace Corporation to rapidly transfer lessons learned and respond to program anomalies. Most importantly, Aerospace is uniquely independent and is not subject to any schedule or cost pressures.

The Aerospace Corporation and the Air Force have found the independent launch verification process extremely valuable. Aerospace Corporation involvement in Air Force launch verification has significantly reduced engineering errors, resulting in a 2.9 percent "probability-of-failure" rate for expendable launch vehicles, compared to 14.6 percent in the commercial sector.[39]

Conclusion

The practices noted here suggest that responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority. Organizations that successfully operate high-risk technologies have a major characteristic in common: they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule and mission-accomplishment goals. The Naval Reactors Program, SUBSAFE program, and the Aerospace Corporation are examples of organizations that have invested in redundant technical authorities and processes to become highly reliable.

7.4 Organizational Causes: A Broken Safety Culture

Perhaps the most perplexing question the Board faced during its seven-month investigation into the *Columbia* accident was "How could NASA have missed the signals the foam was sending?" Answering this question was a challenge. The investigation revealed that in most cases, the Human Space Flight Program is extremely aggressive in reducing threats to safety. But we also know – in hindsight – that detection of the dangers posed by foam was impeded by "blind spots" in NASA's safety culture.

From the beginning, the Board witnessed a consistent lack of concern about the debris strike on *Columbia*. NASA managers told the Board "there was no safety-of-flight issue" and "we couldn't have done anything about it anyway." The investigation uncovered a troubling pattern in which Shuttle Program management made erroneous assumptions about the robustness of a system based on prior success rather than on dependable engineering data and rigorous testing.

184 REPORT VOLUME I AUGUST 2003

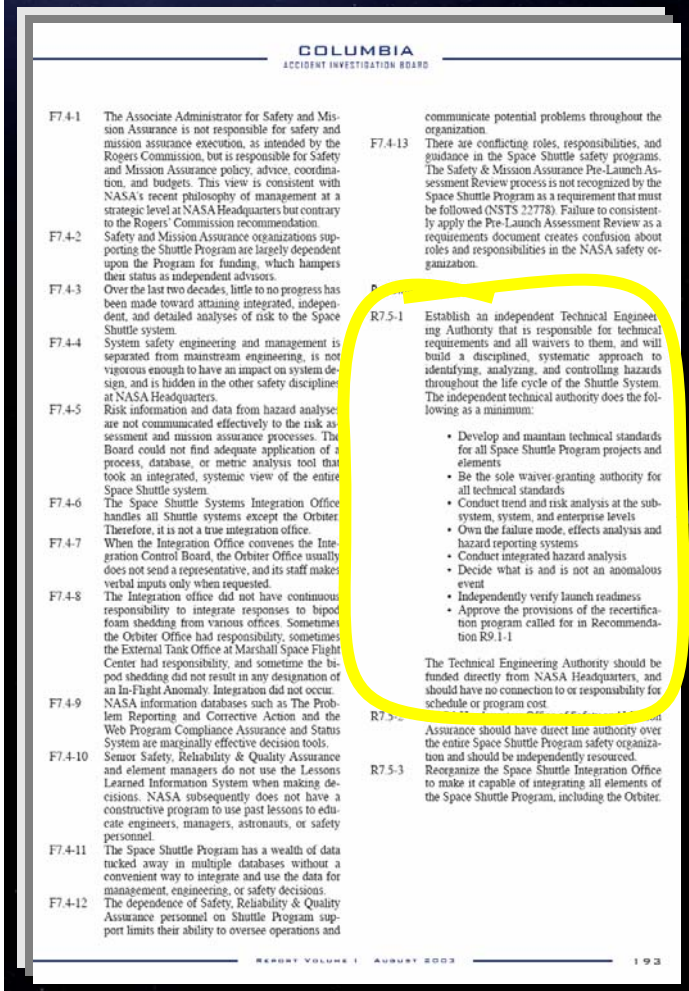
"The practices noted here suggest that responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority."

"Organizations that successfully operate high-risk technologies have a major characteristic in common: they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule and mission-accomplishment goals."

"The Naval Reactors Program, SUBSAFE program and the Aerospace Corporation are examples of organizations that have invested in redundant technical authorities and processes to become highly reliable."

Excerpted from:
CAIB Report Volume 1, Chapter 7.3

CAIB Recommendation 7.5-1



COLUMBIA
ACCIDENT INVESTIGATION BOARD

F7.4-1 The Associate Administrator for Safety and Mission Assurance is not responsible for safety and mission assurance execution, as intended by the Rogers Commission, but is responsible for Safety and Mission Assurance policy, advice, coordination, and budgets. This view is consistent with NASA's recent philosophy of management at a strategic level at NASA Headquarters but contrary to the Rogers' Commission recommendation.

F7.4-2 Safety and Mission Assurance organizations supporting the Shuttle Program are largely dependent upon the Program for funding, which hampers their status as independent advisors.

F7.4-3 Over the last two decades, little to no progress has been made toward attaining integrated, independent, and detailed analyses of risk to the Space Shuttle system.

F7.4-4 System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.

F7.4-5 Risk information and data from hazard analyses are not communicated effectively to the risk assessment and mission assurance processes. The Board could not find adequate application of a process, database, or metric analysis tool that took an integrated, systemic view of the entire Space Shuttle system.

F7.4-6 The Space Shuttle Systems Integration Office handles all Shuttle systems except the Orbiter. Therefore, it is not a true integration office.

F7.4-7 When the Integration Office convenes the Integration Control Board, the Orbiter Office usually does not send a representative, and its staff makes verbal inputs only when requested.

F7.4-8 The Integration office did not have continuous responsibility to integrate responses to bipod foam shedding from various offices. Sometimes the Orbiter Office had responsibility, sometimes the External Tank Office at Marshall Space Flight Center had responsibility, and sometime the bipod shedding did not result in any designation of an In-Flight Anomaly. Integration did not occur.

F7.4-9 NASA information databases such as The Problem Reporting and Corrective Action and the Web Program Compliance Assurance and Status System are marginally effective decision tools.

F7.4-10 Senior Safety, Reliability & Quality Assurance and element managers do not use the Lessons Learned Information System when making decisions. NASA subsequently does not have a constructive program to use past lessons to educate engineers, managers, astronauts, or safety personnel.

F7.4-11 The Space Shuttle Program has a wealth of data tucked away in multiple databases without a convenient way to integrate and use the data for management, engineering, or safety decisions.

F7.4-12 The dependence of Safety, Reliability & Quality Assurance personnel on Shuttle Program support limits their ability to oversee operations and communicate potential problems throughout the organization.

F7.4-13 There are conflicting roles, responsibilities, and guidance in the Space Shuttle safety programs. The Safety & Mission Assurance Pre-Launch Assessment Review process is not recognized by the Space Shuttle Program as a requirement that must be followed (NSTS 22778). Failure to consistently apply the Pre-Launch Assessment Review as a requirements document creates confusion about roles and responsibilities in the NASA safety organization.

R7.5-1 Establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, and will build a disciplined, systematic approach to identifying, analyzing, and controlling hazards throughout the life cycle of the Shuttle System. The independent technical authority does the following as a minimum:

- Develop and maintain technical standards for all Space Shuttle Program projects and elements
- Be the sole waiver-granting authority for all technical standards
- Conduct trend and risk analysis at the subsystem, system, and enterprise levels
- Own the failure mode, effects analysis and hazard reporting systems
- Conduct integrated hazard analysis
- Decide what is and is not an anomalous event
- Independently verify launch readiness
- Approve the provisions of the recertification program called for in Recommendation R9.1-1

The Technical Engineering Authority should be funded directly from NASA Headquarters, and should have no connection to or responsibility for schedule or program cost.

Assurance should have direct line authority over the entire Space Shuttle Program safety organization and should be independently resourced.

R7.5-3 Reorganize the Space Shuttle Integration Office to make it capable of integrating all elements of the Space Shuttle Program, including the Orbiter.

REPORT VOLUME I AUGUST 2003 193

Excerpted from:
Recommendations,
CAIB Report Volume 1, Chapter 7.6

R7.5-1: Establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, and will build a disciplined, systematic approach to identifying, analyzing and controlling hazards throughout the life cycle of the Shuttle System. The independent technical authority does the following as a minimum.

- **Develop and maintain technical standards for all Space Shuttle Program projects and elements**
- **Be the sole waiver-granting authority for all technical standards**
- **Conduct trend and risk analysis at the sub-system, system, and enterprise levels**
- **Own the failure mode, effects analysis and hazard reporting systems**
- **Conduct integrated hazard analysis**
- **Decide what is and is not an anomalous event**
- **Independently verify launch readiness**
- **Approve the provisions of the recertification program called for in Recommendation R9.1-1.**

The Technical Engineering Authority should be funded directly from NASA Headquarters, and should have no connection to or responsibility for schedule or program cost.

Balance of Power

Technical Authority Definition

- Technical Authority is the authority, responsibility, and accountability to establish, approve, and maintain technical requirements, processes, and policy

- NASA is establishing the Technical Authority as a direct response to CAIB Recommendation 7.5-1

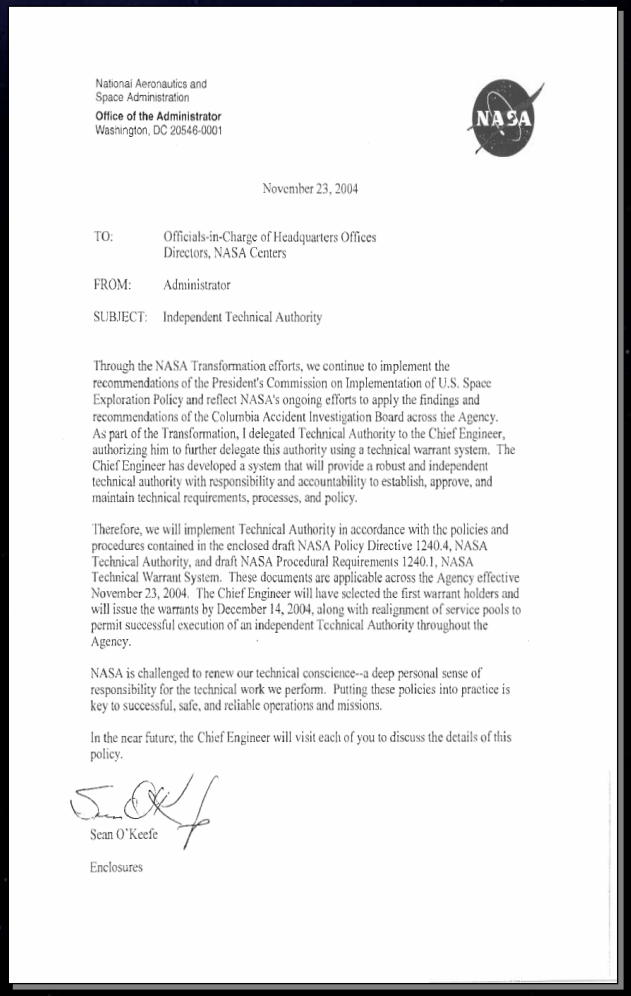
Technical Authority owns the decision on what is technically acceptable in matters involving safe and reliable operations.

Technical Authority Principles*

1. Resides in an individual (Chief Engineer), not an organization,
2. Clear and unambiguous,
3. Independent of the Program Manager,
4. Credible (based on knowledge, experience, resources, personnel pipeline), and
5. Visible and accepted as valid, i.e. has influence and prestige.

* Each separately necessary, but not sufficient in isolation.

ITA Timeline



National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

November 23, 2004

TO: Officials-in-Charge of Headquarters Offices
Directors, NASA Centers

FROM: Administrator

SUBJECT: Independent Technical Authority

Through the NASA Transformation efforts, we continue to implement the recommendations of the President's Commission on Implementation of U.S. Space Exploration Policy and reflect NASA's ongoing efforts to apply the findings and recommendations of the Columbia Accident Investigation Board across the Agency. As part of the Transformation, I delegated Technical Authority to the Chief Engineer, authorizing him to further delegate this authority using a technical warrant system. The Chief Engineer has developed a system that will provide a robust and independent technical authority with responsibility and accountability to establish, approve, and maintain technical requirements, processes, and policy.

Therefore, we will implement Technical Authority in accordance with the policies and procedures contained in the enclosed draft NASA Policy Directive 1240.4, NASA Technical Authority, and draft NASA Procedural Requirements 1240.1, NASA Technical Warrant System. These documents are applicable across the Agency effective November 23, 2004. The Chief Engineer will have selected the first warrant holders and will issue the warrants by December 14, 2004, along with realignment of service pools to permit successful execution of an independent Technical Authority throughout the Agency.

NASA is challenged to renew our technical conscience--a deep personal sense of responsibility for the technical work we perform. Putting these policies into practice is key to successful, safe, and reliable operations and missions.

In the near future, the Chief Engineer will visit each of you to discuss the details of this policy.

Sean O'Keefe

Enclosures

- 26 Months since Columbia Accident
- 20 Months since Release of CAIB Report
- 10 Months since NPR 1000.3A Issued
- ITA Plan Vetted with External Groups
- Administrator Memo approval of policy in November 2004
- 29 Technical Warrants selected
- Warrant Holder Workshops in January and March
  - ITA Declared Standing
- RTF Scheduled for May 2005

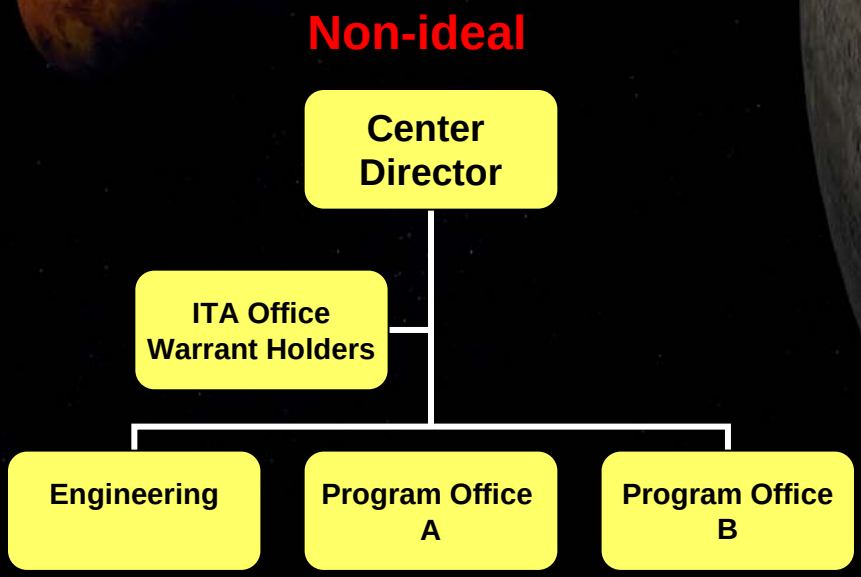
Technical Authority is…

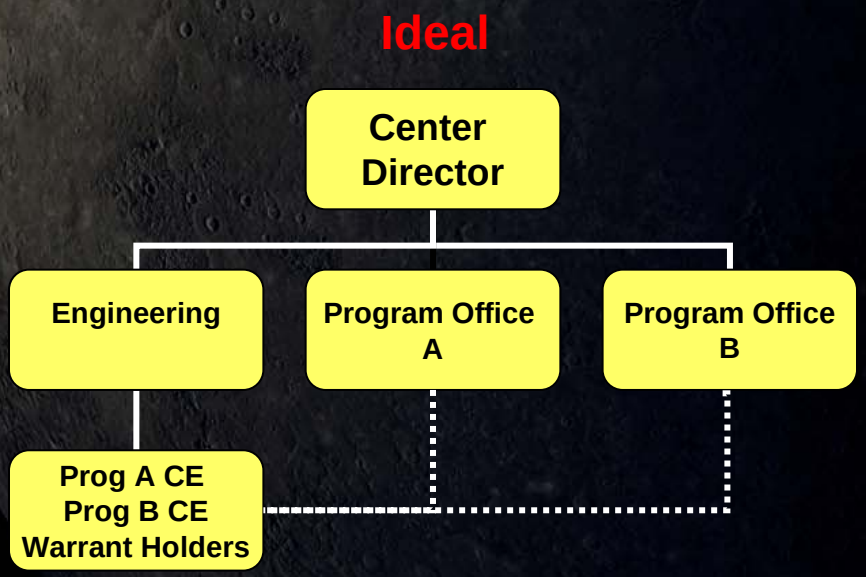
- independent of programmatic authority
  - organizationally & financially
- executed in support of programs and projects to provide
  - adequate checks and balances to ensure safety and reliability,
  - engineering and technical requirements,
  - a disciplined, formal process, standardized across the Agency, for technical requirements and decision making, and
- organic to programs/projects
- centralized
- individualized
- dependent on a balance of power

Technical Authority is the
"technical conscience".

Technical Authority is not…

- a shadow engineering organization
- a shadow program office
- NESC or any sort of independent *assessment*
- a distributed authority—only one ITA
- Mount Olympus





Technical Warrants

- **The Chief Engineer, NASA Technical Authority for Engineering, will issue warrants including:**
  - **Discipline Technical Warrants**
    - **Establish, approve and maintain technical requirements (i.e. specifications, standards, processes, procedures) for their assigned technical discipline.**
  - **Systems Warrant Holders**
    - **Establish, approve and maintain the technical requirements for the system integration of a total vehicle or program system. These Warrant Holders will utilize Warrant Holders in particular technical areas and disciplines, as required and appropriate.**

Technical Warrant Holder

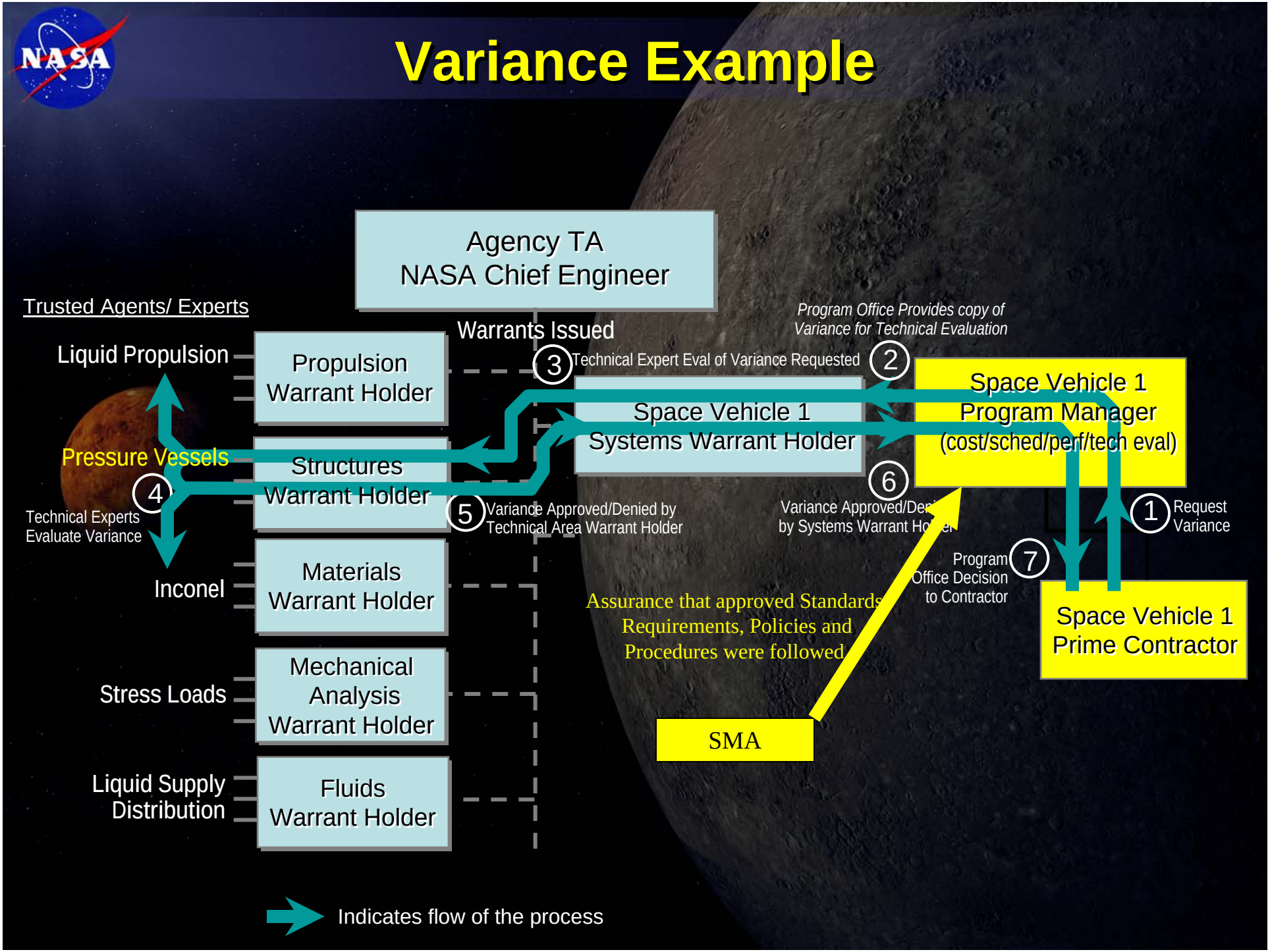
- **Responsibilities**
  - Establishing and maintaining technical requirements,
  - Approving changes and/or variances to technical requirements,
  - Maintaining individual technical expertise,
  - Ensuring products capable of safe and reliable operations,
  - Making unbiased, independent technical decisions,
  - Using sound technical rationale, and
  - Being accountable for technical decisions.

- **Independence**
  - Organizationally, will not report to program or project managers,
  - Are not dependent on Program funding, and
  - Have a direct line to the Agency's Technical Authority via the Warrant, without going through Programs.

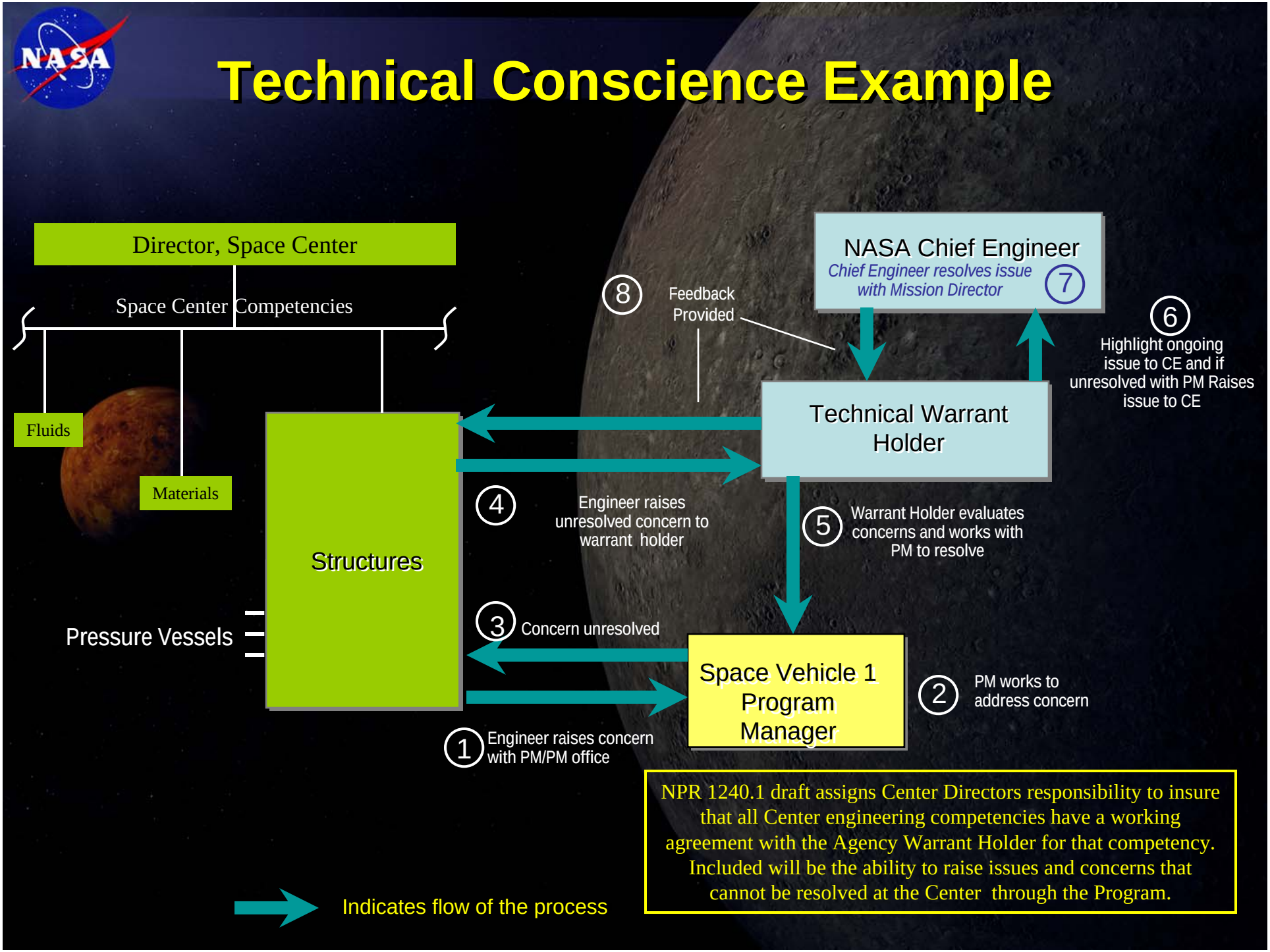
Relationship to Programs

- In order to ensure safe and reliable operations/ missions:
  - Program/ Project Managers (PMs) will comply with the technical requirements and decisions issued by Technical Warrant Holders (TWHs).
  - The TWH will provide PMs and other NASA users with technical requirements as well as ranges of technically acceptable alternatives with risk and value assessments where appropriate.
  - PMs will insure TWH has real time access to all technical information from programs.
  - TWH will issue technical resolution of changes and/ or variances in a timely manner.

Variance Example



Technical Conscience Example



NPR 1240.1 draft assigns Center Directors responsibility to insure that all Center engineering competencies have a working agreement with the Agency Warrant Holder for that competency. Included will be the ability to raise issues and concerns that cannot be resolved at the Center through the Program.

Summary

- Technical Authority is requirement for NASA to continue to effectively and safely conduct the Nation's Space activities.
- The Agency is responding positively to the change.
  - Leadership Support is essential to
    - implement successfully
    - inculcate "technical conscience"
    - make this a way of doing business
- ITA is standing up.

"We do not know where this journey will end, yet we know this: human beings are headed into the cosmos." President Bush